

REMARKS

Reconsideration of this application in light of the amendments and the following remarks is respectfully requested.

Status of the Claims

Claims 1-14 and 16-20 are pending. Claim 15 was previously canceled without prejudice or disclaimer of the subject matter contained therein. Claims 1-6, 11, and 16-19 have been amended. No new matter has been added.

Claim Objections

The Examiner has objected to claims 1, 4, 5, and 6 as containing informalities. Applicants have amended claims 1, 4, 5, and 6 in response to the Examiner's objections. Applicants respectfully request reconsideration and withdrawal of the objections to claims 1, 4, 5, and 6.

Claim Rejections under 35 U.S.C. § 112

Claims 1-5, 11, and 16-19 stand rejected under 35 U.S.C. § 112 "as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention." (Office Action, item 4, page 4.) Applicants have amended each claims 1-5, 11, and 16-18 to address the issues identified by the Examiner.

With respect to claim 19, the Examiner contends that there is insufficient antecedent basis for the limitation of "the step of activating a probe." (Office Action, item 5, page 6, ¶ 3.)

Applicants respectfully disagree. This phrase is in the context of “[t]he method according to claim 6 . . . **further comprising the step of** activating a probe engine.” Thus, this is the first recitation of “activating a probe,” and does not lack antecedent basis.

The Examiner also objects to the last sentence of claim 1, “outputting a list of the detected metric,” as being vague and confusing with respect to the scenario in which only one metric is detected. Applicants respectfully note that claim 1 recites “detecting at least one metric related to at least one of the accessible data sources; . . . outputting a list **of the at least one** detected metric.” A list should be constructed if more than one metric is detected, and if only one metric is detected, the list can contain only one item (i.e., metric). Thus, Applicants respectfully submit that “outputting a list” is appropriate even if only one metric is detected.

Applicants respectfully request reconsideration and withdrawal of this rejection.

Rejection under 35 U.S.C. §102

Claims 1-14 and 16-20 stand rejected under 35 U.S.C. §102(e) as being anticipated by U.S. Patent No. 6,633,835 to Moran et al (“Moran”).

The present invention is directed to a “computer implemented system for managing and monitoring one or more computer systems comprising: a computer . . . configured to receive monitoring information from the one or more computer systems,” as recited by claim 1.

The Examiner contends that Moran teaches “collecting data from a network segment to monitor remotely installed applications and service offerings in real-time,” and “remote network management agents collecting such information.” (Detailed Action, item 8, page 15.) The Examiner further notes that “network traffic is in fact monitored information,” and the claims do not

clarify the phrase “monitoring information.” (Detailed Action, item 8, page 14 (internal quotations omitted).) Thus, the Examiner concludes there is no difference between Moran and the claimed invention.

Applicants submit that Moran discloses a system through which “[d]ata is collected from a **network segment** and classified into multiple flows.” (Moran, col. 2, lines 8-9 (emphasis added).) The “monitoring system 120 is coupled to a network 108,” and includes “one or more media modules [that] . . . **provide a physical observation point of network traffic** on a given segment 306.” (Moran, col. 4, lines 37-38; Moran, col. 5, lines 31-14 (emphasis added.)) Further, Applicants submit that the remote network management (RMON) probes are similarly limited to collecting data from a network segment. (See http://www.cisco.com/univercd/cc/td/doc/cisintwk/ito_doc/rmon.htm (Appendix A) (“*Remote Monitoring (RMON)* is a standard monitoring specification that enables various **network monitors** and console systems to exchange **network-monitoring data**.”); and see Moran, col. 5, lines 37-59)

Thus, Moran monitors and analyzes **network traffic** and does not obtain monitoring information from identified data sources on the network computer systems to determine the operation of the computer systems.

Applicants have amended claim 1 to recite that “the monitoring information concern[s] the operation of the one or more respective computer systems.” Thus, the monitoring information of claim 1 is not information collected by listening to network segments, nor is it information received from remote monitoring (“RMON”) agents that collect data from remote network segments. Rather, the monitoring information “may include status, throughput, performance, configuration, business,

accuracy, availability, security, utilization, geographical, and usability information.” (Specification, page 2, lines 5-7.)

In response to Applicants previous remarks, submitted in the November 3, 2006 Amendment, the Examiner contends that the feature of “scan[ning] the computers attached to the network to detect data sources providing monitoring information” is not recited in the rejected claims. (Detailed Action, item 8, page 15.) The Examiner further notes that regardless of whether the claims recite this feature, Moran teaches this feature by disclosing monitoring agents that collect and provide monitoring information. (Detailed Action, item 8, page 15.)

Applicants respectfully submit that claim 1 explicitly recites, “scanning said one or more computer systems based on the instructions acquired from the configuration to generate a list of the accessible data sources in said scanned computer systems.” Furthermore, as discussed above, the remote monitoring agents disclosed by Moran merely relay network data from a network segment. Moran does not disclosing scanning computers to detect data sources. The data source of Moran is a network segment, it does not reside on, nor is it provided by, a remote computer.

Therefore, for at least the reasons discussed above, Applicants submit that Moran neither discloses nor suggests each and every feature recited in claim 1. Therefore, Moran does not anticipate the invention of claim 1.

Claims 2-5 and 17-18 depend from claim 1. Applicants submit that claims 2-5 and 17-18 are patentable for at least the same reasons as discussed above with respect to claim 1. Reconsideration and withdrawal of the rejection is respectfully requested.

Independent claim 6 recites features that are substantially similar to those features of claim 1 demonstrated above to be missing from Moran. Further, claim 6 recites the step of “collecting from

at least one of said computer systems meta and performance information of said accessible data sources of at least one of said at least one computer system.” The Examiner contends that Moran discloses collecting meta data and performance information in column 37, line 56 bridging column 58, line 30. However, as discussed above, Moran is only capable of collecting information by monitoring traffic on network segments. (Moran, column 37, lines 49-50 (“performance data is gathered during the **monitoring** of operation 3702”).) Moran does not collect information from data sources accessible on the computer systems.

Thus, Applicants submit that Moran does not disclose or suggest the invention recited in claim 6.

Claims 7-14, 16, and 19-20 depend from independent claim 6. Applicants submit that claims 7-14, 16, and 19-20, by virtue of their dependency from claim 6, are patentable for at least the reasons as discussed above.

Applicants respectfully request reconsideration and withdrawal of the rejection.

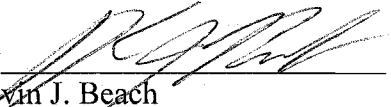
CONCLUSION

Each and every point raised in the Final Office Action dated January 24, 2007 has been addressed on the basis of the above amendments and remarks. In view of the foregoing it is believed that claims 1-14 and 16-20 are in condition for allowance and it is respectfully requested that the application be reconsidered and that all pending claims be allowed and the case passed to issue.

If there are any other issues remaining which the Examiner believes could be resolved through a Supplemental Response or an Examiner's Amendment, the Examiner is respectfully requested to contact the undersigned at the telephone number indicated below.

Dated: June 25, 2007

Respectfully submitted,

By 

Kevin J. Beach

Registration No.: 60,422

DARBY & DARBY P.C.

P.O. Box 5257

New York, New York 10150-5257

(212) 527-7700

(212) 527-7701 (Fax)

Attorney For Applicant

APPENDIX A

Cisco Documentation

[Home](#) [Contents](#) [Previous](#) [Next](#) [Glossary](#) [Feedback](#) [Search](#) [Help](#)

Table Of Contents

[Chapter Goals](#)
[Remote Monitoring](#)
[Background](#)
[RMON Groups](#)
[Review Questions](#)



Chapter Goals

- Describe the background of Remote Monitoring.
- Describe the nine RMON groups of monitoring.

Remote Monitoring

Background

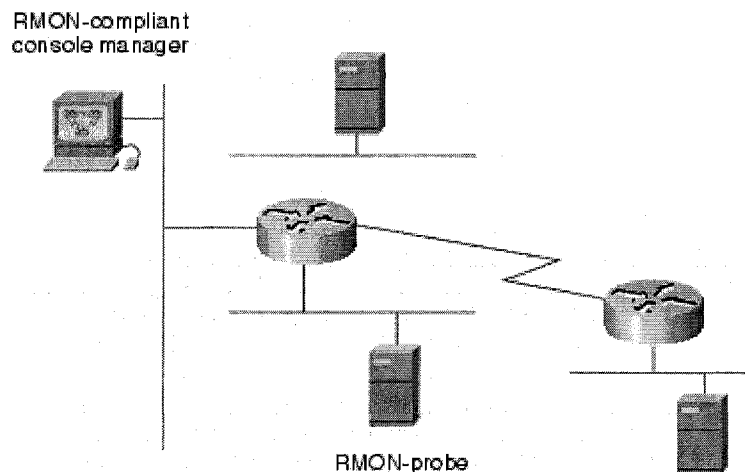
Remote Monitoring (RMON) is a standard monitoring specification that enables various network monitors and console systems to exchange network-monitoring data. RMON provides network administrators with more freedom in selecting network-monitoring probes and consoles with features that meet their particular networking needs. This chapter provides a brief overview of the RMON specification, focusing on RMON groups.

The RMON specification defines a set of statistics and functions that can be exchanged between RMON-compliant console managers and network probes. As such, RMON provides network administrators with comprehensive network-fault diagnosis, planning, and performance-tuning information.

RMON was defined by the user community with the help of the Internet Engineering Task Force (IETF). It became a proposed standard in 1992 as RFC 1271 (for Ethernet). RMON then became a draft standard in 1995 as RFC 1757, effectively obsoleting RFC 1271.

Figure 55-1 illustrates an RMON probe capable of monitoring an Ethernet segment and transmitting statistical information back to an RMON-compliant console.

Figure 55-1 An RMON Probe Can Send Statistical Information to an RMON Console



RMON Groups

RMON delivers information in nine RMON groups of monitoring elements, each providing specific sets of data to meet common network-monitoring requirements. Each group is optional so that vendors do not need to support all the groups within the Management Information Base (MIB). Some RMON groups require support of other RMON groups to function properly. Table 55-1 summarizes the nine monitoring groups specified in the RFC 1757 Ethernet RMON MIB.

Table 55-1 RMON Monitoring Groups

RMON Group	Function	Elements
Statistics	Contains statistics measured by the probe for each monitored interface on this device.	Packets dropped, packets sent, bytes sent (octets), broadcast packets, multicast packets, CRC errors, runts, giants, fragments, jabbers, collisions, and counters for packets ranging from 64 to 128, 128 to 256, 256 to 512, 512 to 1024, and 1024 to 1518 bytes.
History	Records periodic statistical samples from a network and stores them for later retrieval.	Sample period, number of samples, items sampled.
Alarm	Periodically takes statistical samples from variables in the probe and compares them with previously configured thresholds. If the monitored variable crosses a threshold, an event is generated.	Includes the alarm table and requires the implementation of the event group. Alarm type, interval, starting threshold, stop threshold.
Host	Contains statistics associated with each host discovered on the network.	Host address, packets, and bytes received and transmitted, as well as broadcast, multicast, and error packets.
HostTopN	Prepares tables that describe the hosts that top a list ordered by one of their base statistics over an interval specified by the management station. Thus, these statistics are rate-based.	Statistics, host(s), sample start and stop periods, rate base, duration.
Matrix	Stores statistics for conversations between sets of two addresses. As the device detects a new conversation, it creates a new entry in its table.	Source and destination address pairs and packets, bytes, and errors for each pair.
RMON Group	Function	Elements
Filters	Enables packets to be matched by a filter equation. These matched packets form a data stream that might be captured or that might generate events.	Bit-filter type (mask or not mask), filter expression (bit level), conditional expression (and, or not) to other filters.
Packet Capture	Enables packets to be captured after they flow through a channel.	Size of buffer for captured packets, full status (alarm), number of captured packets.
Events	Controls the generation and notification of events from this device.	Event type, description, last time event sent.

Review Questions

Q—What is the function of the RMON group Matrix?

A—This group stores statistics for conversations between sets of two addresses. As the device detects a

new conversation, it creates a new entry in its table.

Q—What is RMON?

A—Remote Monitoring (RMON) is a standard monitoring specification that enables various network monitors and console systems to exchange network-monitoring data.

Q—Multicast packets, CRC errors, runts, giants, fragments, and jabbers are elements of what RMON group?

A—Statistics.

[Home](#) [Contents](#) [Previous](#) [Next](#) [Glossary](#) [Feedback](#) [Search](#) [Help](#)

Posted: Thu Oct 12 21:41:16 PDT 2006

All contents are Copyright © 1992–2006 Cisco Systems, Inc. All rights reserved.

[Important Notices](#) and [Privacy Statement](#).